

ABSTRACT

Network devices such as intrusion detection systems, routers, firewalls, servers, and other network devices are monitored to aggregate all event data generated by monitored devices to provide a threat ranking of all network activity. A threat level for a given host is determined by a threat weighting assigned to that host and a threat weighting assigned to that host's netblock. In addition, a vulnerability for a given event is determined by the event's destination threat associated with a vulnerability value indexed by the event's destination and the event's type.

10